

WHAT IS CLAIMED IS:

1           1.       A method for processing data packets sent through a network, comprising:  
2           receiving data packets from a host through the network wherein the received packets  
3       were, prior to receipt, encrypted and fragmented after encryption;  
4           reassembling the fragmented packets using a communication protocol offload engine in  
5       a network adaptor coupling a host central processing unit to the network;  
6           decrypting the reassembled packets of encryption using a security offload engine in the  
7       network adaptor; and  
8           forwarding the decrypted and reassembled packets to the communication protocol  
9       offload engine.

1           2.       The method of claim 1 further comprising:  
2           receiving from a remote host through the network additional packets which were  
3       encrypted in a first encryption, fragmented after the first encryption and encrypted in a second  
4       encryption after the fragmentation;  
5           decrypting the fragmented packets of the second encryption of using the security  
6       offload engine;  
7           reassembling the fragmented packets decrypted of the second encryption using a  
8       communication protocol offload engine;  
9           decrypting the reassembled packets of the first encryption using the security offload  
10       engine; and  
11          forwarding the decrypted and reassembled additional packets to the communication  
12       protocol offload engine.

1           3.       The method of claim 1, further comprising:

2 receiving from a remote host through the network additional packets which were  
3 encrypted and fragmented after all encryption;  
4 reassembling the fragmented additional packets using the communication protocol  
5 offload engine;  
6 decrypting the reassembled additional packets of encryption using the security offload  
7 engine; and  
8 forwarding the decrypted and reassembled additional packets to the communication  
9 protocol offload engine.

1 4. The method of claim 1, further comprising:  
2 receiving from a remote host through the network additional packets which were  
3 fragmented and then encrypted;  
4 decrypting the fragmented additional packets of encryption using the security offload  
5 engine; and  
6 reassembling the fragmented and decrypted additional packets using the  
7 communication protocol offload engine.

1 5. The method of claim 1, further comprising:  
2 receiving from a remote host through the network additional packets which were  
3 fragmented but not encrypted;  
4 reassembling the fragmented and unencrypted packets using the communication  
5 protocol offload engine.  
6

1 6. The method of claim 1, further comprising:  
2 receiving from a remote host through the network additional packets which were  
3 encrypted but not fragmented;

4        decrypting the unfragmented packets of encryption using the security offload engine;  
5    and  
6        forwarding the decrypted additional packets to the communication protocol offload  
7    engine.

1        7.        The method of claim 2, wherein the first encryption is a transport mode  
2    encryption and the second encryption is a tunnel mode encryption.

1        8.        The method of claim 1, further comprising:  
2        feeding the received packets through a feedforward path from a network interface  
3    receiver in the network adaptor, through the security offload engine and to the communication  
4    protocol offload engine to be reassembled; and  
5        feeding the reassembled packets from the communication protocol offload engine  
6    through a feedback path from the communication protocol offload engine to the security offload  
7    engine to be decrypted.

1        9.        The method of claim 8, wherein said forwarding comprises:  
2        feeding the decrypted and reassembled packets through the feedforward path from the  
3    security offload engine to the communication protocol offload engine; said method further  
4    comprising:  
5        extracting a data payload from the decrypted and reassembled packets using the  
      communication protocol offload engine.

1        10.        The method of claim 8, further comprising:  
2        multiplexing a flow of data packets in the feedforward path from the network interface  
3    receiver to the security offload engine and a flow of data packets in the feedback path from the  
4    communication protocol offload engine to the security offload engine.

5

6

1 11. A network adaptor for use with a network, comprising:

2 a security offload engine having an input and an output and adapted to decrypt

3 encrypted packets;

4 a communication protocol offload engine having an input and an output and adapted to

5 reassemble fragmented packets;

6 a network interface receiver having an output coupled to the security offload engine

7 input and an input adapted to receive from the network packets which were, prior to receipt,

8 encrypted and fragmented after encryption;

9 a feedforward path coupling said receiver output to said security offload engine input

10 and said security offload engine output to said communication protocol offload engine input;

11 a feedback path coupling said communication protocol offload engine output to said

12 security offload engine input; and

13 logic adapted to feed the fragmented packets from the network interface receiver

14 through the feedforward path to the communication protocol offload engine to be reassembled

15 in the communication protocol offload engine, to feed the reassembled packets from the

16 communication protocol offload engine through the feedback path to the security offload engine

17 to be decrypted in the security offload engine, and to feed the decrypted and reassembled

18 packets from the security offload engine, through the feedforward path to the communication

19 protocol offload engine.

1 12. The adaptor of claim 11:

2 wherein said receiver is adapted to receive from the network additional packets which

3 were encrypted in a first encryption, fragmented after the first encryption and encrypted in a

4 second encryption after the fragmentation; and

5            wherein the logic is adapted to to feed the fragmented packets of the second  
6 encryption from the network interface receiver through the feedforward path to the security  
7 offload engine to be decrypted of the second encryption in the security offload engine; to feed  
8 the fragmented packets decrypted of the second encryption from the security offload engine  
9 through the feedforward path to the communication protocol offload engine to be reassembled  
10 in the communication protocol offload engine, to feed the reassembled packets of the first  
11 encryption from the communication protocol offload engine through the feedback path to the  
12 security offload engine to be decrypted of the first encryption in the security offload engine, and  
13 to feed the decrypted and reassembled additional packets packets from the security offload  
14 engine, through the feedforward path to the communication protocol offload engine.

1            13.        The adaptor of claim 11:  
2            wherein said receiver is adapted to receive from the network additional packets which  
3 were encrypted and fragmented after all encryption; and  
4            wherein the logic is adapted to to feed the fragmented additional packets from the  
5 network interface receiver through the feedforward path to the communication protocol offload  
6 engine to be reassembled in the communication protocol offload engine, to feed the  
7 reassembled additional packets from the communication protocol offload engine through the  
8 feedback path to the security offload engine to be decrypted in the security offload engine, and  
9 to feed the decrypted and reassembled additional packets packets from the security offload  
10 engine, through the feedforward path to the communication protocol offload engine.

1            14.        The adaptor of claim 11:  
2            wherein said receiver is adapted to receive from the network additional packets which  
3 were fragmented and then encrypted; and  
4            wherein the logic is adapted to to feed the fragmented additional packets from the  
5 network interface receiver through the feedforward path to the security offload engine to be

6 decrypted in the security offload engine, and to feed the decrypted additional packets packets  
7 from the security offload engine, through the feedforward path to the communication protocol  
8 offload engine.

1 15. The adaptor of claim 11:  
2 wherein said receiver is adapted to receive from the network additional packets which  
3 were fragmented but not encrypted; and  
4 wherein the logic is adapted to to feed the fragmented additional packets from the  
5 network interface receiver through the feedforward path to the communication protocol offload  
6 engine to be reassembled in the communication protocol offload engine.

7  
1 16. The adaptor of claim 11:  
2 wherein said receiver is adapted to receive from the network additional packets which  
3 were encrypted but not fragmented; and  
4 wherein the logic is adapted to to feed the encrypted additional packets from the  
5 network interface receiver through the feedforward path to the security offload engine to be  
6 decrypted of the encryption in the security offload engine, and to feed the decrypted and  
7 additional packets packets from the security offload engine, through the feedforward path to  
8 the communication protocol offload engine.

1 17. The adaptor of claim 12 wherein the first encryption is a transport mode  
2 encryption and the second encryption is a tunnel mode encryption.

1 18. The adaptor of claim 11 the communication protocol offload engine is adapted  
2 to extracting a data payload from the decrypted and reassembled packets.

1           19.     The adaptor of claim 11 wherein the feedback path and the feedforward path  
2 includes a multiplexor adapted to multiplex a flow of data packets in the feedforward path from  
3 the network interface receiver output to the security offload engine input and a flow of data  
4 packets in the feedback path from the communication protocol offload engine output to the  
5 security offload engine input.

1           20.     The adaptor of claim 11 wherein the feedback path includes a buffer wherein  
2 said logic is adapted to store reassembled packets from the communication protocol offload  
3 engine to await multiplexing by said multiplexor to the security offload engine input.

1           21.     A system for use with a network, comprising:  
2           a system memory;  
3           a processor coupled to the system memory;  
4           data storage coupled to the processor and the system memory;  
5           a data storage controller adapted to manage Input/Output (I/O) access to the data  
6 storage; and  
7           a network adaptor which includes:  
8           a security offload engine coupled to the memory and having an input and an output and  
9 adapted to decrypt encrypted packets;  
10          a communication protocol offload engine having an input and an output and adapted to  
11 reassemble fragmented packets;  
12          a network interface receiver having an output coupled to the security offload engine  
13 input and an input adapted to receive from the network packets which were, prior to receipt,  
14 encrypted and fragmented after encryption;  
15          a feedforward path coupling said receiver output to said security offload engine input  
16 and said security offload engine output to said communication protocol offload engine input;

17           a feedback path coupling said communication protocol offload engine output to said  
18 security offload engine input; and  
19           logic adapted to feed the fragmented packets from the network interface receiver  
20 through the feedforward path to the communication protocol offload engine to be reassembled  
21 in the communication protocol offload engine, to feed the reassembled packets from the  
22 communication protocol offload engine through the feedback path to the security offload engine  
23 to be decrypted in the security offload engine, and to feed the decrypted and reassembled  
24 packets from the security offload engine, through the feedforward path to the communication  
25 protocol offload engine.  
26  
27

28           22.     An article of manufacture for use with a network wherein the article of  
29 manufacture causes operations to be performed, the operations comprising:  
30                   receiving data packets from a remote host through the network wherein the  
31 received packets were, prior to receipt, encrypted and fragmented after encryption;  
32                   reassembling the fragmented packets using a communication protocol offload engine in  
33 a network adaptor coupling a host central processing unit to the network;  
34                   decrypting the reassembled packets of encryption using a security offload engine in the  
35 network adaptor; and  
36                   forwarding the decrypted and reassembled packets to the communication protocol  
37 offload engine.

1           23.     The article of manufacture of claim 22, wherein the operations further comprise:  
2                   receiving from a remote host through the network additional packets which were  
3 encrypted in a first encryption, fragmented after the first encryption and encrypted in a second  
4 encryption after the fragmentation;



5            decrypting the fragmented packets of the second encryption of using the security  
6 offload engine;  
7            reassembling the fragmented packets decrypted of the second encryption using a  
8 communication protocol offload engine;  
9            decrypting the reassembled packets of the first encryption using the security offload  
10 engine; and  
11           forwarding the decrypted and reassembled additional packets to the communication  
12 protocol offload engine.

1           24.    The article of manufacture of claim 22, wherein the operations further comprise:  
2           receiving from a remote host through the network additional packets which were  
3 encrypted and fragmented after all encryption;  
4           reassembling the fragmented additional packets using the communication protocol  
5 offload engine;  
6           decrypting the reassembled additional packets of encryption using the security offload  
7 engine; and  
8           forwarding the decrypted and reassembled additional packets to the communication  
9 protocol offload engine.

1           25.    The article of manufacture of claim 22, wherein the operations further comprise:  
2           receiving from a remote host through the network additional packets which were  
3 fragmented and then encrypted;  
4           decrypting the fragmented additional packets of encryption using the security offload  
5 engine; and  
6           reassembling the fragmented and decrypted additional packets using the  
7 communication protocol offload engine.

1           26.    The article of manufacture of claim 22, wherein the operations further comprise:  
2           receiving from a remote host through the network additional packets which were  
3   fragmented but not encrypted;  
4           reassembling the fragmented and unencrypted packets using the communication  
5   protocol offload engine.

1           27.    The article of manufacture of claim 22, wherein the operations further comprise:  
2           receiving from a remote host through the network additional packets which were  
3   encrypted but not fragmented;  
4           decrypting the unfragmented packets of encryption using the security offload engine;  
5   and  
6           forwarding the decrypted additional packets to the communication protocol offload  
7   engine.

1           28.    The article of manufacture of claim 23, wherein the first encryption is a  
2   transport mode encryption and the second encryption is a tunnel mode encryption.

1           29.    The article of manufacture of claim 22, wherein the operations further comprise:  
2           feeding the received packets through a feedforward path from a network interface  
3   receiver in the network adaptor, through the security offload engine and to the communication  
4   protocol offload engine to be reassembled; and  
5           feeding the reassembled packets from the communication protocol offload engine  
6   through a feedback path from the communication protocol offload engine to the security offload  
7   engine to be decrypted.

1           30.    The article of manufacture of claim 29, wherein said forwarding operation  
2   comprises:

3 feeding the decrypted and reassembled packets through the feedforward path from the  
4 security offload engine to the communication protocol offload engine; and  
5 wherein the operations further comprise extracting a data payload from the decrypted  
and reassembled packets using the communication protocol offload engine.

1 31. The article of manufacture of claim 22, wherein the operations further comprise:  
2 multiplexing a flow of data packets in the feedforward path from the network interface  
3 receiver to the security offload engine and a flow of data packets in the feedback path from the  
4 communication protocol offload engine to the security offload engine.

1 32. The system of claim 21, wherein the logic is further adapted to:  
2 multiplex a flow of data packets in the feedforward path from the network interface  
3 receiver to the security offload engine and a flow of data packets in the feedback path from the  
4 communication protocol offload engine to the security offload engine.

1 33. An adaptor, comprising:  
2 a network interface controller adapted to receive fragments of network packets, at least  
3 some of the fragments originating from network packets encrypted prior to fragmentation;  
4 a communication protocol offload engine to reassemble the network packets from the  
5 received fragments;  
6 a security offload engine to decrypt at least a portion of the reassembled network  
7 packets to provide decrypted packets; and  
8 logic adapted to selectively return at least some of the decrypted packets to the  
9 communication protocol offload engine.

- 1           34.     The adaptor of claim 33 wherein the communication protocol of the
- 2     communication protocol offload engine is the Transmission Control Protocol (TCP) and
- 3     Internet Protocol (IP).